EXHIBIT 3

1 PACIFIC TRIAL ATTORNEYS
   A Professional Corporation
2 Scott J. Ferrell, Bar No. 202091
   sferrell@pacifictrialattorneys.com
3 4100 Newport Place Drive, Ste. 800
   Newport Beach, CA 92660
4 Tel: (949) 706-6464
   Fax: (949) 706-6469
5
   Attorneys for Plaintiff
6

7

8   **SUPERIOR COURT FOR THE STATE OF CALIFORNIA**

9   **COUNTY OF LOS ANGELES**

10

11 MARIELITA PALACIOS,   Case No. 24STCV11264

12   Plaintiff,   **FIRST AMENDED COMPLAINT FOR**
                                           VIOLATION OF CALIFORNIA INVASION
13   v.   **OF PRIVACY ACT ("CIPA")**

14 FANDOM, INC., a Delaware corporation, with its
    principal place of business in California, d/b/a   Assigned Judge: Hon. Joseph Lipner
15 WWW.FANDOM.COM,   Dept: 72

16   Defendant.   Complaint filed: May 6, 2024
                                           Trial date: TBA
17

18

19

20

21

22

23

24

25

26

27

28

I.   INTRODUCTION

Defendant has secretly deployed spyware at www.fandom.com/ (the "Website") that accesses visitors' devices and installs tracking spyware prior to any efforts to obtain consent to do so, and then monitors and reports visitors' online habits *after* they leave the Website.

Plaintiff recently visited Defendant's Website.   Without Plaintiff's knowledge or consent, Defendant secretly accessed Plaintiff's device and installed "pen register" and "trap and trace" tracking software in violation of California law.   The harm caused by this intrusion is grave, as summarized by the world's leading cybersecurity firm:

> "*Data is worth money, which is a major reason that your online privacy is under threat.*
>
> *For instance, knowing your browsing habits or search history can deliver big profits to advertisers. If you've been searching for new apartments, your search history could tip an advertiser off to the fact that you're going to be moving home soon — time to start serving you ads for moving services, furniture, DIY stores, and home insurance….*
>
> *The risks are more far-reaching than most people realize because of what might happen to your data next. The development of Big Data means that your browsing history could be analyzed to come up with conclusions that you don't want to be drawn. For example, a woman buying items such as folic acid supplements might not appreciate a marketing agency identifying her as 'pregnant' and targeting her with pregnancy products. [¶] If she's living with mom and dad or hasn't told her partner, she might not be happy to see 'Congratulations on Your Baby!' marketing materials arrive in the mail….*
>
> *Whenever you visit a website, data is being stored about you — possibly without your consent and even without your knowledge. You likely want to know where that data goes and how it's used, or you could decide you want to avoid it being collected altogether.*"[1]

II.   JURISDICTION AND VENUE

1.   Defendant is subject to jurisdiction in this state under Penal Code section 502(j), which provides that a person who accesses a computer from another jurisdiction is deemed to have personally

---

[1]   Excerpted from "***What Is Data Privacy?***", found online at https://usa.kaspersky.com/resource-center/threats/internet-and-individual-privacy-protection (last visited Apr. 18, 2024) (emphasis added).

1   accessed the computer in California. Plaintiff was in California when Defendant accessed Plaintiff's

2   device and installed tracking code.

3   2.   Defendant is also subject to jurisdiction under California's "long-arm" statute found at

4   California Code of Civil Procedure section 410.10 because the exercise of jurisdiction over Defendant

5   is not "inconsistent with the Constitution of this state or the United States." Indeed, Plaintiff is informed

6   and believes and thereon alleges that Defendant generates a minimum of eight percent of revenues from

7   its Website based upon interactions with Californians (including instances in which the Website operates

8   as a "gateway" to sales), such that the website "is the equivalent of a physical store in California." Since

9   this case involves Defendant's activities in the forum state, California courts can "properly exercise

10   personal jurisdiction" over the Defendant in accordance with the Court of Appeal opinion in *Thurston

11   v. Fairfield Collectibles of Georgia*, 53 Cal. App. 5th 1231, 1235 (2020).

12   3.   Venue is proper in this County pursuant to California Code of Civil Procedure section

13   394(b).

III.   PARTIES

15   4.   Plaintiff is a resident of California. Plaintiff is also a consumer privacy advocate who

16   works as a "tester" to ensure that companies abide by the privacy obligations imposed by California

17   law. As an individual who advances important public interests at the risk of vile personal attacks,

18   Plaintiff should be "praised rather than vilified." *See Murray v. GMAC Mortgage Corp*., 434 F.3d 948,

19   954 (7th Cir. 2006). Indeed, the Ninth Circuit recently made exceptionally clear that it is "necessary

20   and desirable for committed individuals to bring serial litigation" to enforce and advance consumer

21   protection statutes, and that Courts must not make any impermissible credibility or standing inferences

22   against them. *Langer v. Kiser*, 57 F.4th 1085, 1095 (9th Cir. 2023).

23   5.   Defendant is a corporation incorporated in the state of Delaware with a principal place of

24   business in California. Defendant is a media fandom platform with users of its Website throughout the

25   United States including the state of California and this County.

IV.   FACTUAL ALLEGATIONS

27   **A.   The Right to Privacy Has Always Been a Legally Protected Interest in the United States.**

28

6.   Since America's founding, privacy has been a legally protected interest at the local, state, and federal levels. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271–72 (9th Cir. 2019) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)) ("Privacy rights have long been regarded 'as providing a basis for a lawsuit in English or American courts.'"); and *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) ("Violations of the right to privacy have long been actionable at common law.").

7.   More specifically, privacy protections against the disclosure of personal information are embedded in California statutes and at common law. *See e.g.*, *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) ("The Ninth Circuit has repeatedly held that privacy intrusions may constitute "concrete injury" for purposes of Article III standing); *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1041–43 (9th Cir. 2017) (finding "concrete injury" where plaintiffs claimed that unsolicited telemarketing calls "invade the privacy and disturb the solitude of their recipients*"); In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 599 (9th Cir. 2020) (finding "concrete injury" where Facebook allegedly tracked users' "personally identifiable browsing history" on third party websites), *cert. denied*, 141 S. Ct. 1684 (2021); *Patel*, 932 F.3d at 1275 (finding "concrete injury" where plaintiffs claimed Facebook's facial-recognition technology violated users' privacy rights).

8.   In short, the privacy of personal information is—and has always been—a legally protected interest in many contexts. Thus, a defendant whose acts or practices violate consumer privacy inflicts an actionable "injury" upon an individual.

B.   The California Invasion of Privacy Act

9.   The California Legislature enacted the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 *et seq.*, to protect certain privacy rights of California citizens. The California Legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." (Cal. Penal Code § 630.)

10.   As relevant here, section 638.51(a) proscribes any "person" from "install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order."

FIRST AMENDED COMPLAINT

11.   A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." (Cal. Penal Code § 638.50(b).)

12.   A "trap and trace device" is "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." (Cal. Penal Code § 638.50(b).)

13.   In plain English, a "pen register" is a "device or process" that records *outgoing* information, whereas a "trap and trace device" is a "device or process" that records *incoming* information. A "pen register" and "trap and trace device" are collectively referred to herein as "Pen-Traps" or "PR/TT".

14.   Historically, law enforcement used "pen registers" to record the numbers of outgoing calls from a particular telephone line, while law enforcement used "trap and trace devices" to record the numbers of incoming calls to that particular telephone line. As technology advanced, however, courts have expanded the application of those surveillance devices consistent with changes in both federal and state law.

15.   For example, with the passage of the 2001 USA PATRIOT Act, the Pen-Trap definition was expanded to include a device or process to keep up with the advancement and evolution of Internet technologies and communications. In 2015, the California Legislature overwhelmingly adopted this updated and expanded definition without a single vote in opposition. *See* Stats. 2015, ch. 204, § 1 (A.B. 929) (eff. Jan. 1, 2016); *see also In re Order Authorizing Prospective & Continuous Release of Cell Site Location Recs.*, 31 F. Supp. 3d 889, 898 n.46 (S.D. Tex. 2014) (citing *Susan Freiwald*, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949, 982-89 (1996) (describing the evolution of PR/TT technology from mechanical device to computer system)).

16.   For example, if a user sends an email, a "pen register" might record the email address it was sent from, the email address that the email was sent to, and the subject line—because this is the user's *outgoing* information. On the other hand, if the same user receives an email, a "trap and trace

FIRST AMENDED COMPLAINT

1 device" might record the email address it was sent from, the email address it was sent to, and the subject

2 line—because this is *incoming* information that is being sent to that same user.

3   17.   Although CIPA was enacted before the dawn of the Internet, "the California Supreme

4 Court regularly reads statutes to apply to new technologies when such a reading would not conflict with

5 the statutory scheme." *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *21 (N.D.

6 Cal. Sept. 26, 2013); *see also Greenley v. Kochava*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023)

7 (referencing CIPA's "expansive language" when finding software was a "pen register"); *Javier v.

8 Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of

9 wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This accords with the fact

10 that "when faced with two possible interpretations of CIPA, the California Supreme Court has construed

11 CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v.

12 Google Inc.*, No. 15-CV-04062-LHK, 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

13   18.   Individuals may bring an action against the violator of any provision of CIPA—including

14 section 638.51 of the Penal Code—for $5,000 per violation. (Cal. Penal Code § 637.2(a)(1).)

15   19.   CIPA provides for a private right of action and imposes civil liability and statutory

16 penalties for the installation of pen register or trap and trace device without a court order. Cal. Penal

17 Code § 637.2; *see also Greenley*, 684 F. Supp. 3d at 1050-51. In *Greenley*, the federal district court

18 denied a motion to dismiss in a materially identical case, noting the "expansive language in the

19 California Legislature's chosen decision," *id.* at 1050, which the court held was specific as to the type

20 of data a pen register collects – DRAS – but "vague and inclusive as to the form of the collection tool –

21 'a device or process.'" *Id.* The *Greenley* court concluded that the language suggests that "courts should

22 focus less on the form of the data collector and more on the result." *Id.* Having this legal framework in

23 mind, the court applied the plain meaning to the word "process" and concluded that "software that

24 identifies consumers, gathers data, and correlates that data through unique 'fingerprinting'" is a process

25 that falls within CIPA's "pen register" definition. *Id.*

26 **C.   Website Operators Can Deploy Tracking Software to De-Anonymize Otherwise

27   Anonymous Website Visitors and Track and Surveil Such Users.**

28

FIRST AMENDED COMPLAINT

20.   Individuals who use devices to connect to an Internet website are typically anonymous and expect to remain anonymous. Some rogue website operators, however, secretly attach a "tracking beacon" to visitor devices that are then used to track and surveil users.

21.   The tracking software will connect fragments of information – such as a unique IP address, user's operating system name, operating system version number, browser name, browser version number, browser language, screen resolution, geolocation data, email address, mobile ad IDs, embedded social media identities, customer and/or loyalty IDs, cookies and device signature – with connections between them. The tracking software also connects and correlates "undeclared identifiers", such as membership in an email or subscriber list, demographics, purchases/transactions, visits to online news sites, survey results, voter registration, and motor vehicle records.

22.   Using tracking software, a website owner can correlate a grouping of fragments and the connections between them to create a unique digital profile of each individual website visitor. This process is known as "digital fingerprinting."

23.   If a website owner can link a unique digital profile created by digital fingerprinting to a particular individual, the website owner can assemble a detailed picture of a person's private life, including: the online services for which an individual has registered; personal interests based on websites visited; organizational affiliations; where the individual has been physically; a person's political and religious affiliations; individuals with whom they have leanings and with whom they associate; and where they travel, among other things. *See* https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/ (last visited Apr. 18, 2024).

24.   Digital fingerprinting of a website's users allows the website owner or its agent to monitor user activity (such as page views, searches, or purchases), de-codes the device used by each website visitor, and enables a website to identify the location, race, age, preferences, internet browsing history, and ethnicity of each user. This data is captured and processed for the purpose of identifying the source of electronic communications on the website for consumer identification purposes.

25.   The following graphic shows how a website deploying digital fingerprinting spyware has gathered and assimilated the digital fingerprints of a website visitor to create a unique digital identifier and link it to a previously anonymous individual named Mary Smith, thereby revealing a treasure trove

FIRST AMENDED COMPLAINT

of private information about Mary Smith's private life:

26.   In the above example, identity resolution has been achieved: using spyware materially identical to the technology used by the Defendant, the website owner has gathered and assimilated sufficient digital fingerprints of an anonymous visitor to identify that visitor as Mary Smith, and now knows the following information about her:

(a) Full name *(Mary Smith)*

(b) Date of birth *(May 1, 1979)*

(c) Gender *(female)*

(d) Home address *(2345 Avenue C, Papillion Nebraska)*

(e) Marital Status and Family *(Married with two children)*

(f) E-mail address *(*Mary.Smith@gmail.com*)*

(g) Personal Cell Phone: *(111) 123-4567*

(h) Voter Registration Status *(Registered)*

(i) Interests *(Shopping, Cooking, Traveling, Reading, Science)*

(j) Employer *(Karen's Fireside, Inc.)*

(k) Title *(Vice President)*

(l) Work Hours *(Daily 9-5)*

FIRST AMENDED COMPLAINT

27.   For the preceding reasons, the ability to link a unique digital profile to a specific individual using digital fingerprinting is of great monetary value. Indeed, it has created an entire industry known as "identity resolution." Identity resolution is generally defined as "the ability to recognize an individual person, in real-time, by connecting various identifiers from their digital interactions across devices and touchpoints." *See* https://www.fullcontact.com/identity-resolution/ (last visited Apr. 18, 2024).

28.   One of the means by which a website owner can gather digital fingerprints as part of its identity resolution efforts is by deploying Pen-Traps spyware on its website.

29.   In lay terms, PR/TT spyware captures electronic impulses that identify the originating source of Internet communication by capturing routing, address, or signaling information. One means of doing so is to secretly deploy tracking spyware on a website.

30.   Indeed, PR/TT spyware has caught the attention of the United States Director of National Intelligence, who recently explained that "the advancement of digital technology, including location-tracking and other features of smartphones and other electronic devices, and the advertising-based monetization models that underlie many commercial offerings available on the Internet" pose a threat to the individuals and "raises significant issues related to privacy and civil liberties."

D.   The PR/TT Spyware Is a "Pen Register".

31.   To make Defendant's Website load on a user's internet browser, the browser sends an "HTTP request" or "GET" request to Defendant's server where the relevant Website data is stored. In response to the request, Defendant's server sends an "HTTP response" back to the browser with a set of instructions. *See* Figure 1.
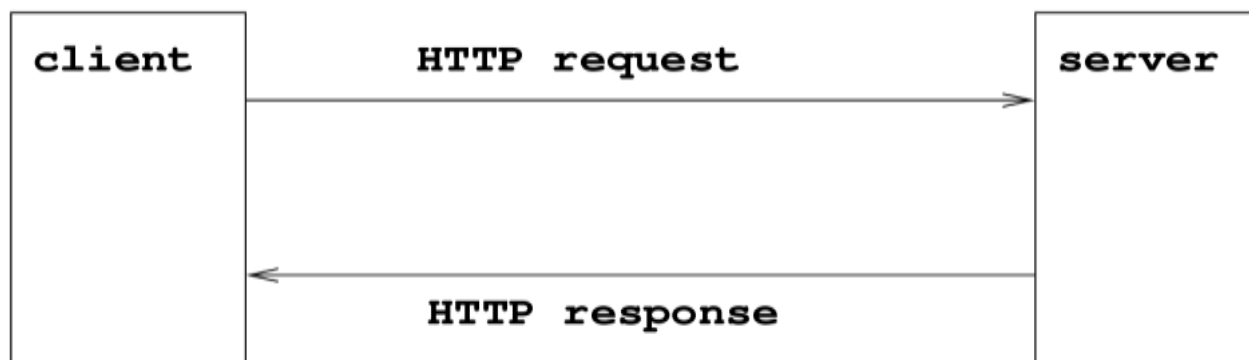
Figure 1:

/ / /

/ / /

/ / /

/ / /

FIRST AMENDED COMPLAINT

32.   The server's instructions include how to properly display the Website—*e.g.*, what images to load, what text should appear, or what music should display.

33.   In addition, the server's instruction cause at least one PR/TT beacon to be installed on a Website user's Internet browser. The PR/TT beacon then causes the browser to send identifying information—including the user's IP address—to the PR/TT beacon's software provider, which is a software-as-a-service company that develops the PR/TT beacon provided to website owners like Defendant for a fee. The PR/TT beacon's software provider uses such PR/TT beacon to receive, store, and analyze data collected from website visitors, including visitors of Defendant's Website. The PR/TT beacon's software provider provides analytics and marketing services to Defendant using the data collected from visitors to the Website when they visited the Website and from when they visited other websites that included the PR/TT beacon.

34.   The IP address is a unique identifier for a device, which is expressed as four sets of numbers separated by periods (*e.g.*, 192.168.123.132). The first two sets of numbers indicate what network the device is on (*e.g.*, 192.168), and the second two sets of numbers identify the specific device (*e.g.*, 123.132).

35.   Thus, the IP address enables a device to communicate with another device—such as a computer's browser communicating with a server—and the IP address contains the device's geographical location.

36.   Through an IP address, the device's state, city, and zip code can be determined.

37.   As alleged below, Defendant installs the PR/TT beacon on the user's browser, and such PR/TT beacon collects information—users' IP addresses—that identifies the outgoing "routing,

FIRST AMENDED COMPLAINT

addressing, or signaling information" of the user. Accordingly, Defendant's PR/TT beacon is a "pen register."

38.   The first time a user visits Defendant's Website, the user's browser sends an HTTP request to Defendant's server, and Defendant's server sends the HTTP response. This response also includes directions to install the PR/TT beacon on the user's browser. The PR/TT beacon, in turn, instructs the user's browser to send the user's IP address to the PR/TT beacon's developer.

39.   Moreover, the PR/TT beacon's developer stores a beacon or cookie with the user's IP address in the user's browser cache. When the user subsequently visits Defendant's Website, the PR/TT beacon instructs the user's browser to send the user's IP address through the beacon or cookie.

40.   If the user clears his or her cookies, then the user wipes out the PR/TT beacon from the user's browser cache. Accordingly, the next time the user visits Defendant's Website, the process begins over again: (i) Defendant's server installs the PR/TT beacon on the user's browser, (ii) the PR/TT beacon instructs the browser to send to the PR/TT developer the user's IP address, (iii) the PR/TT beacon stores a beacon or cookie in the browser cache, and (iv) the PR/TT beacon's developer will continue to receive the user's IP address on subsequent visits to the Website through the cookie or beacon.

41.   In all cases, the PR/TT beacon receives a user's IP address each and every time a user interacts with the website of one of the PR/TT beacon's developer's clients, including Defendant's Website.

42.   The user's IP address is transmitted to the PR/TT beacon along with the cookie value.

43.   The PR/TT beacon is at least a "process" because it is "software that identifies consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050.

44.   Further, the PR/TT beacon is a "device" because "in order for software to work, it must be run on some kind of computing device. It is artificial to claim that software must be viewed in isolation from the computing device on which it runs and with which it is inseparable in regard to the challenged conduct." *James v. Walt Disney Co.*, - F. Supp. 3d -, No. 23-cv-02500-EMC (EMC), 2023 WL 7392285, at *13 (N.D. Cal. Nov. 8, 2023).

FIRST AMENDED COMPLAINT

45.   Because the PR/TT beacon captures the outgoing information—the IP address—from visitors to websites, it is a "pen register" for the purposes of section 638.50(b) of the California Penal Code.

E.   Defendant Secretly Installed Tracking Software on Plaintiff's and Other Users' Browsers Without Prior Consent or a Court Order in Violation of California Law.

46.   Defendant owns and operates the Website.

47.   When companies build their websites, they install or integrate various third-party scripts into the code of the website in order to collect data from users or perform other functions.[2]

48.   Oftentimes, third-party scripts are installed on websites "for advertising purposes." *Id.*

49.   Further, "[i]f the same third-party tracker is present on many sites, it can build a more complete user profile over time." *Id.*

50.   Defendant has incorporated the code of the PR/TT beacon into the code of its Website. Thus, when Plaintiff visited the Website, the Website caused the PR/TT beacon to be installed on Plaintiff's and other users' browsers.

51.   As outlined above, when a user visits the Website, the Website's code—as programmed by Defendant—installs the PR/TT onto the user's browser.

52.   Upon installing the PR/TT on its Website, Defendant uses the PR/TT to collect the IP address of visitors to the Website, which is used by the PR/TT beacon's developer to provide services to Defendant and its other clients, including targeted advertisements and website analytics. Defendant and its partners use the PR/TT beacon to "digitally fingerprint" each visitor.

53.   At no time prior to the installation and use of the PR/TT beacon on Plaintiff's and other users' browsers, or prior to the use of the PR/TT beacon, did Defendant procure Plaintiff's or other users' consent for such conduct. Nor did Defendant obtain a court order to install or use the PR/TT

---

[2] "Third-party tracking refers to the practice in which a tracker on a website is set by a different website than the one the visitor is currently on. Third-party trackers are snippets of code that are typically installed on multiple websites. They collect and send information about a user's browsing history to other companies, often for advertising purposes. If the same third-party tracker is present on many sites, it can build a more complete user profile over time." https://piwik.pro/glossary/third-party-tracking/ (last visited Apr. 18, 2024). "[C]ompanies may be in trouble using third-party cookies on their websites without complying with privacy laws in a specific jurisdiction…." *Id.*

FIRST AMENDED COMPLAINT

1   beacon. The PR/TT beacon deploys prior to any efforts to notify visitors or obtain their consent to being

2   tracked.

3   54.   The specific PR/TT spyware beacons detected on Defendant's Website are identified

4   below, which explains the details of the beacons' deployment and the breadth of the beacons' operation.

5   Plaintiff's investigation of the Website has determined that at least four types of PR/TT spyware are

6   deployed by the Website, *i.e.*, Nexxen, Audigent/Hadron, CrazyEgg.com, and Neustar.

7   **1.   Data Harvesting Without Consent**

8   55.   When a user visits the Website, distinct third-party tracking services are detected. These

9   entities, recognized as prominent digital trackers, employ sophisticated methodologies to profile users.

10   These methodologies encompass the acquisition of device IP addresses, synchronizing external

11   identifiers, utilizing TCP/IP header-derived IP addresses, and extracting user agent and device

12   particulars. Additionally, they engage in cookie-sharing practices during request transmissions on the

13   Website.

14   56.   Plaintiff's investigation of the Website via a computer expert has determined that visitor

15   data is harvested and shared with third-party services immediately upon webpage loading, preceding

16   any opportunity for visitors to consent to or decline the Website's privacy policy.

17   57.   Defendant's Website lacks any cookie banner for a visitor to the Website to select any

18   cookie-related preferences upon visiting the Website for the first time.

19   **2.   Nexxen**

20   58.   The Nexxen platform is used for businesses to identify and segment visitors for marketing

21   campaigns. Companies can use the Nexxen platform to buy or sell this audience data.
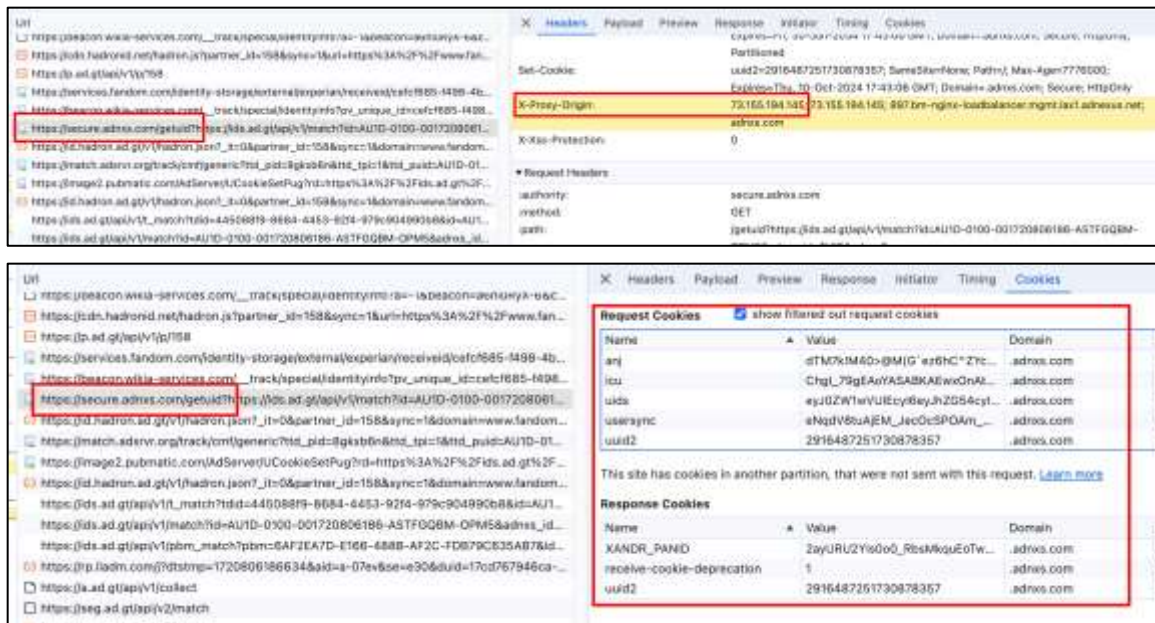
22   / / /

23   / / /

24   / / /

25   / / /

26   / / /

27   / / /

28   / / /

FIRST AMENDED COMPLAINT

59.   A request is sent to the Nexxen tracking URL: adnxs.com. The X-Proxy-Origin in the response header returned by Nexxen contains the visitor's IP address. In addition to IP tracking, the Website enables the use of third-party tracking cookies to be stored on the visitor's browser and sent with the request.

3.   Audigent / Hadron

60.   Audigent / Hadron use cookieless tracking technology, which allows websites like the Website to sell fingerprinted visitors as audience data. The request below shows that the visitor's IP address has been tracked and stored by the server.

FIRST AMENDED COMPLAINT

4. CrazyEgg.com

61.   When a user visits a website that uses Crazy Egg's service, JavaScript tracking code contacts Crazy Egg's servers and enables Crazy Egg to collect and analyze the user's activity while visitors are on the Website. This information is then stored on Crazy Egg's web servers and databases for use in performing analysis and producing reports for Crazy Egg's clients.

62.   Recorded user sessions can be filtered down to a specific individual by providing specific identifiers. For example, if this identifier is an email address, then every action a person took on the website can be viewed.

63.   The request below shows that the visitor's IP address has been tracked and stored by Crazy Egg servers.


5. Neustar

64.   Neustar's Customer Experience services connect data and media across channels (e.g., online, offline, television, etc.) to enable marketers to analyze visitor behavior to create segmented audiences for targeted marketing campaigns.

65.   Visitor devices are fingerprinted, and devices identified as being associated with users are tracked and unified into a single behavioral profile. Tracking is not limited to digital interaction; physical and offline activities are tracked and used to further build a predictive psychological profile for visitors.

66.   The request below contains various visitor identification values and stores tracking cookies on the browser to more easily identify visitors.

FIRST AMENDED COMPLAINT
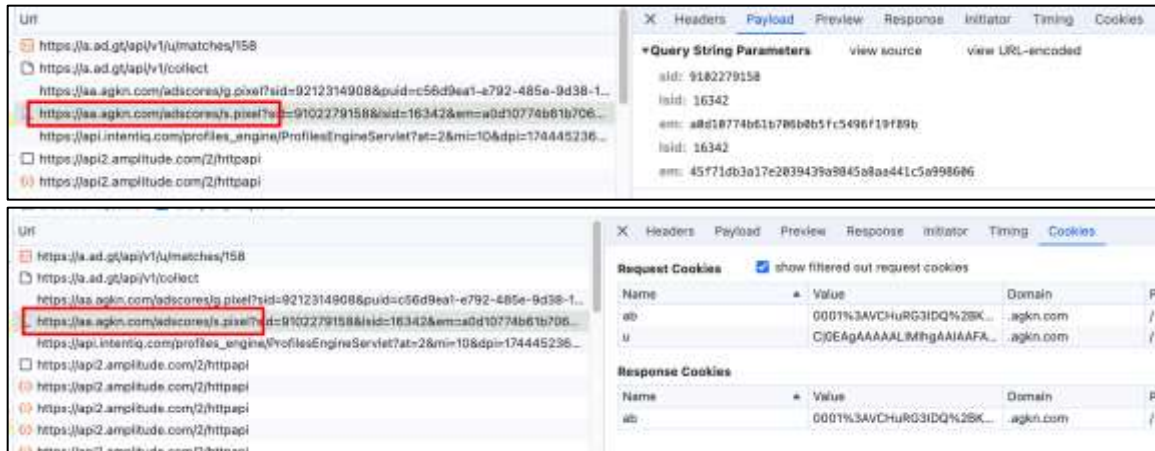
F.   Defendant's Conduct Constitutes an Invasion of Plaintiff's Privacy.

67.   The collection of Plaintiff's personally identifying, non-anonymized information through Defendant's installation and use of the PR/TT beacon constitutes an invasion of privacy.

68.   As alleged herein, the PR/TT beacon is designed to analyze Website data and marketing campaigns, conduct targeted advertising, and boost Defendant's revenue, all through their surreptitious collection of user data including Plaintiff's data.

69.   Companies such as Defendant share their users' data with the PR/TT beacon's developer. In order for such developer to perform data analysis on user data and to assist companies like Defendant to run targeted advertising campaigns, the PR/TT beacon's developer needs to collect data that identifies a particular user. This is why the PR/TT beacon's developer collects IP addresses: it allows the developer to segment users in order to run targeted campaigns and perform data analysis.

70.   In other words, companies like Defendant are collecting users' data and sending it to its PR/TT beacon's developer for a profit including by optimizing its marketing campaigns.

G.   Plaintiff's Experience

71.   Plaintiff has visited the Website within the applicable statute of limitations period via an Internet-connected computer. In particular, Plaintiff's visit occurred in February 2024.

72.   When Plaintiff visited the Website, the Website's code—as programmed by Defendant—caused the PR/TT beacon to be installed on Plaintiff's browser. Defendant and the PR/TT beacon's developer then used the PR/TT beacon to collect Plaintiff's IP address.

FIRST AMENDED COMPLAINT

73.   Defendant and the PR/TT beacon's developer used the information collected by the PR/TT beacon to analyze Website data and marketing campaigns, conduct targeted advertising, and ultimately boost Defendant's and/or advertisers' revenue.

74.   Plaintiff did not provide Plaintiff's prior consent to Defendant to install or use the PR/TT beacon on Plaintiff's browser.

75.   Defendant did not obtain a court order before installing or using the PR/TT beacon.

76.   Plaintiff has, therefore, had Plaintiff's privacy invaded by Defendant's violations of section 638.51(a) of the California Penal Code.

77.   As explained above, Defendant knowingly and intentionally deployed PR/TT spyware to (1) decode and record the routing, addressing, and signaling information transmitted by Plaintiff's electronic device communication; and (2) capture the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication as part of its identity resolution efforts. This conduct constitutes illegal installation of PR/TT spyware in violation of California law.

78.   Defendant did not obtain Plaintiff's knowing and informed consent to the preceding acts, nor did Defendant obtain a court order authorizing it to do so.

79.   **Plaintiff brings this action as an individual Complaint with the hope that Defendant will voluntarily stop its unlawful conduct, remediate the damage caused, and compensate Plaintiff. If Defendant refuses, Plaintiff will amend this Complaint to name additional plaintiffs and/or add class allegations. Plaintiff does not assert any claims arising under federal law.**

V.   CAUSE OF ACTION

CALIFORNIA INVASION OF PRIVACY ACT

PENAL CODE SECTION 638.51(a)

80.   Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein.

81.   Plaintiff brings this cause of action individually against Defendant.

82.   Section 638.51 of the Penal Code provides that it is illegal for any "person' to "install or use a pen register or a trap and trace device without first obtaining a court order pursuant to Section 638.52 or 638.53." (Cal. Penal Code § 638.51(a).)

83.   A "pen register" is a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." (Cal. Penal Code § 638.50(b).)

84.   The PR/TT beacon is a "pen register" because it is a "device or process" that "capture[d]" the "routing, addressing, or signaling information"—the IP address—from the electronic communications transmitted by Plaintiff's computer or smartphone. (Cal. Penal Code § 638.50(b).)

85.   At all relevant times, Defendant knowingly installed the PR/TT beacon—which is a pen register—on Plaintiff's browser, and used the PR/TT beacon to collect Plaintiff's IP address, and track Plaintiff.

86.   The PR/TT beacon does not collect the content of Plaintiff's electronic communications with the Website. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014) ("IP addresses 'constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers.'") (quotation omitted).

87.   Plaintiff did not provide Plaintiff's prior consent to Defendant's installation or use of the PR/TT beacon.

88.   Defendant did not obtain a court order to install or use the PR/TT beacon.

89.   Pursuant to section 637.2 of the California Penal Code, Plaintiff has been injured by Defendant's violation of section 638.51(a) of the California Penal Code, and seeks statutory damages of $5,000 for Defendant's violation of section 638.51(a). *See* Penal Code § 637.2(a)(1).

90.   By knowingly violating a criminal statute and accessing Plaintiff's browser to install tracking software without Plaintiff's prior consent, Defendant acted with oppression and malice. As such, Defendant is liable for punitive damages pursuant to Civil Code section 3294.

PRAYER FOR RELIEF

FIRST AMENDED COMPLAINT

1   WHEREFORE, Plaintiff seeks judgment against Defendant as follows:

2   a.   For statutory damages, punitive damages, reasonable attorneys' fees pursuant to Cal.

3   Civ. Proc. Code § 1021.5, and costs of suit; and

4   b.   For any and all other relief at law that may be appropriate.

5   Dated: July 12, 2024   PACIFIC TRIAL ATTORNEYS, APC

6   By:_____

7   Scott. J. Ferrell
                                                        Attorneys for Plaintiff

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

- 19 -
FIRST AMENDED COMPLAINT

PROOF OF SERVICE
STATE OF CALIFORNIA, COUNTY OF ORANGE

I am employed in the County of Orange, State of California. I am over the age of 18 and not a party to the within action; my business address is 4100 Newport Place Drive, Suite 800, Newport Beach, CA 92660.

On July 12, 2024, I served the foregoing document described as **FIRST AMENDED COMPLAINT FOR VIOLATION OF CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")** on the following person(s) in the manner indicated:

SEE ATTACHED SERVICE LIST

☐   (BY MAIL)   I am familiar with the practice of Pacific Trial Attorneys for collection and processing of correspondence for mailing with the United States Postal Service. Correspondence so collected and processed is deposited with the United States Postal Service that same day in the ordinary course of business. On this date, a copy of said document was placed in a sealed envelope, with postage fully prepaid, addressed as set forth herein, and such envelope was placed for collection and mailing at Pacific Trial Attorneys, Newport Beach, California, following ordinary business practices.

☐   (BY FEDERAL EXPRESS OVERNIGHT)   I am familiar with the practice of Pacific Trial Attorneys for collection and processing of correspondence for delivery by overnight courier. Correspondence so collected and processed is deposited in a box or other facility regularly maintained by Federal Express that same day in the ordinary course of business. On this date, a copy of said document was placed in a sealed envelope designated by Federal Express with delivery fees paid or provided for, addressed as set forth herein, and such envelope was placed for delivery by Federal Express at Pacific Trial Attorneys, Newport Beach, California, following ordinary business practices.

☐   (BY HAND DELIVERY) I am familiar with the practice of Pacific Trial Attorneys for collection and processing of correspondence for hand delivery by courier. I caused such document to be delivered by hand to the addressee(s) designated.

☒   (BY ELECTRONIC SERVICE) I am causing the document(s) to be served by email or electronic transmission via USA Legal sent on the date shown below to the email addresses of the persons listed in the attached service list.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct, and that this declaration was executed on July 12, 2024, at Newport Beach, California.

_____
Mandy K. Jung

PROOF OF SERVICE

SERVICE LIST

Ryan Tyz, Esq.   Attorneys for Defendant
Erin Jones, Esq.   FANDOM, INC.
Deborah Hedley, Esq.
Stephanie Alvarez Salgado, Esq.
Tyz Law Group PC
4 Embarcadero Center, 14th Floor
San Francisco, CA 94111
Email: ryan@tyzlaw.com
Email: ejones@tyzlaw.com
Email: deborah@tyzlaw.com
Email: stephanie@tyzlaw.com

PROOF OF SERVICE